SZYFROWANE DYSKI ODPOWIEDZIĄ NA ZAGROŻENIA ŚRODOWISKA PRACY XXI WIEKU

Coraz większe zagrożenie dla firmy i jej danych stanowią pracownicy używający własnego sprzętu. Czy dyski SSD i pendrive'y z wbudowanym szyfrowaniem sprzętowym stanowią rozwiązanie problemu? ALBO będą rozwiązaniem problemu?

Elastyczność pracy jest jednym z dominujących trendów na rynku w XXI wieku. Siedzenie przy biurku w siedzibie firmy przestaje być nieodłącznym elementem dnia każdego pracownika. Ostatnio coraz częściej widzimy pracowników wykonujących zadania na własnym sprzęcie IT w zaciszu kąta lub w kawiarni. Jest to możliwe dzięki nowoczesnej komunikacji oraz oprogramowaniu. Umożliwia ono pracę osobom przebywającym w różnych miejscach na całym świecie tak jakby siedzieli w jednym pokoju.

Praca zdalna pozytywnie wpływa na produktywność i zadowolenie pracownika. Nowoczesne firmy coraz częściej wybierają ten model biznesowy, ponieważ przynosi on pożądane skutki. Pozwala również ominąć sztywne godziny pracy czy zaoszczędzić na wynajmowaniu przestrzeni biurowej. Ułatwia to pracownikom zachowanie balansu pomiędzy życiem prywatnym a zawodowym. Firmy mają też możliwość wyboru z większej puli ekspertów.

Zmiana ta powoduje również odejście od tradycyjnych stanowisk pracy ze stacjonarnym komputerem. W większości domów mamy bardzo wiele podłączonych urządzeń do sieci za pomocą których pracujemy i łączymy się do sieci i systemów przedsiębiorstwa. Nie tylko jednak pracujemy zdalnie we własnych mieszkaniach, ale często również często podłączamy sprzęt służbowy w miejscach publicznych podczas podróży czy lunchów. Chodzi przede wszystkim o dane przechowywanych na służbowych laptopach, ale dane z firm przenoszone są również na pendrive'ach, tabletach czy nawet kamerach. Rodzi to potencjalne problemy dla bezpieczeństwa. Łączenie urządzeń osobistych z tymi zawierającymi informacje służbowe może mieć opłakane w skutkach konsekwencje i stworzyć nowe ryzyko cyberataków. Jeśli urządzenia zawierające niezaszyfrowane pliki zostaną skradzione to złodziej uzyskuje dostęp do wszystkich danych firmy. Taka sytuacja może mieć poważne skutki dla funkcjonowania organizacji, jej reputacji na rynku, stabilności finansowej czy też skutkować karami za złamanie RODO. Z drugiej jednak strony wprowadzenie zakazu pracy zdalnej będzie krokiem wstecz prowadzącym do spadku wydajności pracownika i jego zadowolenia.

Na szczęście istnieją rozwiązania, która pozwalają firmom na odpowiednie zabezpieczenie danych firmowych, nawet jeżeli znajdują się poza bezpieczną siecią firmową. Odpowiedzią na zagrożenie jest szyfrowanie. Jednak należy pamiętać, że szyfrowanie, szyfrowaniu nie równe. Bezpieczeństwo zależy od metody szyfrowania, która została użyta i zrozumieniu jakie są różnice pomiędzy różnymi technikami szyfrowania. Odpowiednie szkolenia pozwolą pracownikom na zachowanie komfortu pracy, a pracodawcy na zapewnienie bezpieczeństwa danych.

Komputery PC i MAC mają wbudowane oprogramowanie szyfrujące, które może zostać wykorzystane do zabezpieczenia danych. W wypadku kiedy złodziej uzyska fizyczny dostęp do nich nie będzie w

stanie odzyskać ważnych informacji bez podania hasła. Bezpieczeństwo zależy tu jednak w dużej mierze od użytkownika. Jeżeli dane zabezpieczone są słabym, łatwym do odgadnięcia hasłem można stosunkowo prosto uzyskać do nich dostęp. Włączenie oprogramowania szyfrującego na urządzeniach używanych przez pracownika jest prostą metodą na poprawę bezpieczeństwa. O wiele lepszym sposobem jest jednak szyfrowanie na poziomie sprzętu.

Przede wszystkim można je zastosować do pendrive'ów. Ich mały rozmiar powoduje, że łatwo jest je przenosić oraz łatwo można je wpiąć do praktycznie każdego urządzenia. Pojemność tych urządzeń sięgająca 2 terabajtów powoduje, że jest to najlepszy i najwygodniejszy sposób przenoszenia informacji w bezpieczny sposób. Możliwe jest również wykorzystanie urządzenia do tworzenia kopii zapasowych. Jednak niewielkie rozmiary powodują, że bardzo łatwo jest go zgubić, narażając się na utratę krytycznych informacji, które mogą zostać odczytane przez nieuprawnione do tego osoby.

Wbudowane szyfrowanie sprzętowe pozwala jednak na zmniejszenie tego ryzyka. Wykorzystanie 256 bitowego standardu szyfrowania AES (Advanced Encryption Standard) używanego w pendrive'ach pozwoliło na uzyskanie certyfikatu FIPS (Federal Information Processing Standard). Oznacza to, że ktokolwiek znajdzie taki pendrive'a nie będzie miał praktycznie żadnych szans aby dostać się do jego zawartości. Pendrive'y z wbudowanym szyfrowaniem sprzętowym są nieznacznie droższe od swoich niezabezpieczonych kuzynów. Bezpieczeństwo powinno być jednak traktowane jako inwestycja i - potencjalne kary płynące z utraty danych czy straty wizerunkowe mogą być o wiele boleśniejsze niż zakup tego typu sprzętu.

Dyski SSDs z wbudowanym szyfrowaniem sprzętowym zapewniają kompleksową ochroną danych. Używane wewnętrznie lub jako dysk zewnętrzny, dają firmie i jej pracownikom certyfikowany sprzęt o podwyższonym poziomie bezpieczeństwa z lepszymi osiągnięciami niż pendriv'y. Pozwala na przetrzymywanie danych w bezpieczny sposób bez wpływu na jego wydajność czy konieczność ingerencji użytkownika.

Zgoda na wykorzystanie przez pracowników własnych urządzeń jest tanią i łatwą metodą poprawy ich warunków pracy. Jednakże bez podjęcia odpowiednich środków zapobiegawczych, potencjalne ryzyko dla danych przedsiębiorstwa może być bardzo duże. Rozwiązaniem jest jednak wprowadzenie odpowiedniego szyfrowania.